THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

Nicole Toussaint and Veronica Roman, individually and on behalf of all others similarly situated, Plaintiffs, v. HanesBrands, Inc., Defendant.	Case No.: 1:22-cv-00879-LCB-LPA CONSOLIDATED AMENDED CLASS ACTION COMPLAINT Jury Trial Demanded

PLAINTIFFS' CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

Plaintiffs Nicole Toussaint and Veronica Roman ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this action against Defendant HanesBrands, Inc. ("HBI" or "Defendant") to obtain damages, restitution, and injunctive relief for the Class, as defined below. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of the recent data security incident and data breach that was perpetrated against Defendant HBI (the "Data Breach"), which held in its possession certain personally identifiable information ("PII" or "the Private Information") of Plaintiffs and other individuals (the "Class") by Defendant HBI. This Data Breach (a ransomware attack) was first detected by HBI on or around May 24, 2022.

2. The Private Information compromised in the Data Breach included certain highly sensitive personal and protected health information of current and former employees, including Plaintiffs, and other individuals. This Private Information included, but is not limited to: name, address, date of birth, financial account information, government-issued identification numbers such as driver's license, Passport and Social Security number, and other information related to benefits and employment, including sensitive health information collected for employment-related purposes.[1]

3. The Private Information compromised in what HBI refers to as a "data security incident" was copied—*i.e.*, exfiltrated—by cyber-criminals who intentionally targeted HBI for the highly sensitive Private Information it collects, then perpetrated the attack. As a result, the Private Information of Plaintiffs and Class remains in the hands of those cyber-criminals or has been sold on the "dark web" (as HBI admits is a risk that it continues to monitor, *see, e.g.,* Ex. A).

4. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Private Information with which it was entrusted for employment or other business purposes.

5. Plaintiffs bring this class action lawsuit on behalf of themselves and all others similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and

[1] *See, e.g.*, Plaintiff Toussaint's Notice Letter, attached as Exhibit A.

adequate notice to Plaintiffs and other Class Members of exactly what of their Private Information was subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

6. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant HBI's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

7. Defendant disregarded the rights of Plaintiffs and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiffs' and Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members with prompt and full notice of the Data Breach.

8. In addition, Defendant HBI failed to properly monitor the computer network and systems that housed the Private Information. Had HBI properly monitored its property, it would have discovered the intrusion sooner.

9. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant HBI collected and maintained is now in the hands of data thieves.

10. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, filing false medical claims using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

11. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

12. Plaintiffs and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

13. Through this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

14. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including

improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

15. Accordingly, Plaintiffs brings this action against Defendant seeking redress for its unlawful conduct and asserting claims on behalf of a nationwide class for: (i) negligence, (ii) negligence *per se*, (iii) breach of implied contract, (iv) invasion of privacy; (v) unjust enrichment, and (vi) breach of implied covenant of good faith and fair dealing. On behalf of a subclass of California residents, Plaintiff Roman brings a claim for violations of (vii) the California Unfair Business Practices Act.

PARTIES

16. Plaintiff Nicole Toussaint is and at all relevant times was an individual citizen of the State of Maine and a former employee of Defendant. Ms. Toussaint received notice of the Data Breach dated August 16, 2022, attached as Exhibit A.

17. Plaintiff Veronica Roman is and at all relevant times was an individual citizen of the State of California and is a former employee of Defendant. Ms. Roman received notice of the Data Breach dated September 30, 2022, attached as Exhibit B.

18. Defendant HanesBrands, Inc. is a North Carolina Business Corporation company with its principal place of business at 1000 E. Hanes Mill Road, Winston-Salem, North Carolina 27105.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 Class

Members, and at least one Class Member, including both Plaintiffs Nicole Toussaint and Veronica Roman, is a citizen of a state different from Defendant.

20. The Court has personal jurisdiction over Defendant because it is headquartered in this District, has its principal place of business in this District, and regularly conducts business in this District.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in, were directed to and/or emanated from this District, Defendant is based in this District, and maintains Plaintiffs' and Class Members' PII in the District.

FACTUAL ALLEGATIONS

Defendant's Business

22. Defendant HanesBrands, Inc. manufactures and sells apparel under the brand names HBI, Champion, and Bonds. HBI currently employs 59,000 associates in thirty-three countries.[2]

23. HanesBrands, Inc. is one of the world's largest producers of clothing. HanesBrands sells clothing under well-known brand names, including Hanes, Champion, Bali, Berlei, Bonds, Bras N Things, ComfortWash, Gear for Sports, JMS/Just My Size, Maidenform, Playtex, and Wonderbra.

[2] https://www.hanes.com/corporate?section=company (last accessed Apr. 26, 2023).

24. For the purposes of this Class Action Complaint, all of HBI's associated locations and/or subsidiaries that were affected by this Data Breach will be referred to collectively as "HBI."

25. In the ordinary course of employment or seeking employment with Defendant HBI, each applicant and/or employee must provide (and Plaintiffs did provide) Defendant HBI with sensitive, personal, and private information, such as their:

- Name, address, phone number, and email address;
- Date of birth;
- Social Security number;
- Marital status;
- Demographic information;
- Driver's license, and state or federal identification (*e.g.*, Passport);
- Personal health information and disclosures required for job requirements;
- Other personal information related to and necessary to receive employment benefits and employment; and
- Bank account numbers, financial institution, and/or credit card information.

26. Although HBI claims in its Notice Letters that "the safety of [former and current employee] personal information is of the utmost importance to [it],"[3] HBI does not follow its own policies or industry standard practices in securing employee's PII.

[3] *See* Plaintiff Toussaint's Notice Letter, Exhibit A.

27. In its very short and vague "Corporate Privacy Notice," HBI tells its employees (including Plaintiffs and the Class) that: "We maintain reasonable administrative, technical and physical safeguards to protect your Personal Information."[4]

28. Yet, through its failure to properly secure the Private Information of Plaintiffs and Class, HBI has not adhered to its own promises of protecting employees' privacy rights.

29. The current and former employees' (and upon information and belief, employees' dependents') information held by Defendant HBI in its computer system and network included the highly sensitive Private Information of Plaintiffs and Class Members.

The Data Breach

30. A ransomware attack occurs when cyber criminals intend to access a computer system for criminal purposes, then do actually access and steal Private Information (the "Data Breach") that has not been adequately secured by a business entity like HBI.

31. According to the "Notice of Security Incident" that HBI mailed to current and former employees and other affected individuals, *i.e.*, Class members, "[o]n May 24, 2022, [it] detected a ransomware incident impacting certain internal IT systems." Its investigation "recently identified that some of [Class members'] personal information was impacted in the event."[5]

[4] https://www.Hanes.com/corporate?section=company (last accessed Apr. 26, 2023).
[5] *See, e.g.*, Exhibits A and B.

32. However, without further explanation, in its notice letter HBI claims that" "We take the security of all information in our control very seriously."[6] Then it claims to be "tak[ing] a number of steps to even further strengthen the security of our networks." Additionally, HBI tacitly admits that the risks of identity theft are substantial and imminent because it is "continuing to monitor the dark web for any indication of misuse of personal information in connection with this incident . . .." However, HBI does not indicate how it is monitoring the dark web, and whether (or how) it will inform Class members if it discovers (or has already discovered) their stolen Private Information on the dark web.[7]

33. The Notice of Data Security Incident mailed specifically to Plaintiff Toussaint also states that the PII stolen "may have included contact information; date of birth; financial account information; government issued identification numbers such as drivers' license numbers, passport information and social security numbers; and other information related to benefits and employment, including certain limited health information provided for employment-related purposes."[8]

34. As reported to some State Attorneys General in its Data Breach Notifications ("breach report") on May 24, 2022, HBI's investigation revealed that the Private Information (including both PII some limited PHI) of **at least 75,106 individuals** was accessed in this Data Breach.[9]

---

[6] *Id.*
[7] *Id.*
[8] *See* Exhibit A.
[9] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/79cfa377-302d-4c7a-a35a-455237e2b9d0.shtml (last visited Apr. 24, 2023).

35. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice

36. It is well known that PII, including Social Security numbers in particular, is a valuable commodity and a frequent, intentional target of cyber criminals. Companies that collect such information, including HBI, are well aware of the risk of being targeted by cybercriminals.

37. Individuals place a high value not only on their PII, but also on the privacy of that data. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

38. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice, "[a] direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (*e.g.*, postage, phone

calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss."[10]

39. Individuals, like Plaintiffs and Class Members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and is likened to accessing your DNA for hacker's purposes.

40. Data Breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiffs and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse.

41. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[11]

42. In 2021, there were a record 1,862 data breaches, surpassing both the recent record of 1,108 data breaches in 2020, and the previous record of 1,506 set in 2017.[12]

---

[10] "Victims of Identity Theft, 2018," U.S. Dep't of Just. (Apr. 2021, NCJ 256085) available at: https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed Apr. 24, 2023).
[11] https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Apr. 24, 2023).
[12] https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last accessed Apr. 24, 2023).

43. Additionally in 2021, there was a 15.1% increase in cyberattacks and data breaches as compared to 2020. Over the next two years, in a poll done on security executives, they have predicted an increase in attacks from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[13]

44. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, and hopefully can ward off a cyberattack.

45. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data."[14] This publication also explains that "[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."[15]

---

[13] https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 (last accessed Apr. 24, 2023).
[14] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last accessed Apr. 24, 2023).
[15] *Id.*

46. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, HBI failed to take appropriate steps to protect the PII of Plaintiff(s) and the proposed Class from being compromised.

Defendant Fails to Comply with FTC Guidelines

47. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

48. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal employee information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[16] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the

[16] *Protecting Personal Information: A Guide for Business*, FTC (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Apr. 26, 2023).

system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[17]

49. The FTC emphasizes that early notification to data breach victims reduces injuries: "If you quickly notify people that their personal information has been compromised, they can take steps to reduce the chance that their information will be misused" and "thieves who have stolen names and Social Security numbers can use that information not only to sign up for new accounts in the victim's name, but also to commit tax identity theft. People who are notified early can take steps to limit the damage."[18]

50. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[19]

51. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they

[17] *Id*.
[18] https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business (last accessed Apr. 24, 2023).
[19] *See* FTC, *Start With Security*, *supra*.

should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks.

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts

from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

52. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect employee data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

53. Defendant failed to properly implement basic data security practices.

54. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to employees' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

55. Defendant was at all times fully aware of its obligation to protect the PII and of its applicants, past and current employees, their dependents, and other individuals from whom it collected and stored PII. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

56. Several best practices have been identified that a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all employees; utilizing strong passwords; creating multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; using multi-factor authentication; protecting backup data, and; limiting which employees can access sensitive data.

57. Other best cybersecurity practices that are standard in business include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

58. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

59. These foregoing frameworks are existing and applicable industry standards in business, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

Defendant has Breached its Obligations to Plaintiffs and Class

60. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard HBI's computer systems and the Class members' PII stored on its networks. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect past and current employees' and other individuals' Private Information;

c. Failing to properly and continuously monitor its own data security systems for existing intrusions;

d. Failing to ensure that vendors with access to individuals' PII data employed reasonable security procedures;

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

61. As the result of maintaining its computer systems in manner that required security upgrading, inadequate procedures for handling emails containing ransomware or other malignant computer code, and inadequately trained employees who opened files

containing the ransomware virus, Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

62. Accordingly, as outlined below, Plaintiffs and Class Members now face an imminent and substantial risk of fraud and identity theft.

Data Breaches Put Consumers at an Increased Risk Of Fraud and Identify Theft

63. Data Breaches such as the one experienced by HBI's employees and other individuals are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

64. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[20]

65. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

66. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

[20] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Gov't Accountability Office (June 2007), https://www.gao.gov/new.items/d07737.pdf (last visited Oct. 12, 2022) ("GAO Report").

67. Theft of Private Information is also gravely serious. PII is a valuable property right.[21]

68. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

69. There is a strong probability that the entirety of the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

70. In 2019, the United States Government Accountability Office released a report addressing the steps consumers can take after a data breach.[22] Its appendix of steps

[21] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3–4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[22] https://www.gao.gov/assets/gao-19-230.pdf (last accessed Apr. 26, 2023). Attached as Ex. C.

consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. *See* GAO chart of consumer recommendations, reproduced and attached as Exhibit C. It is clear from the GAO's recommendations that the steps Data Breach victims (like Plaintiff(s) and Class) must take after a breach like Defendant's are both time consuming and of only limited and short-term effectiveness.

71. Private Information can sell for as much as $363 per record according to the Infosec Institute.[23] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

72. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[24] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[25] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law

[23] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Apr. 26, 2023).
[24] *Identity Theft and Your Social Security Number* at 1, Social Security Administration (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Apr. 26, 2023).
[25] *Id.* at 4.

enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

73. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[26]

74. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[27]

75. In recent years, employers have experienced disproportionally higher numbers of data theft events than in the past. Defendant therefore knew or should have known of this heightened risk and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

---

[26] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Apr. 24, 2023).

[27] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Apr. 26, 2023).

76. Data breaches are preventable.[28] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[29] She/he/they added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised."[30]

77. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[31]

78. Here, Defendant knew of the importance of safeguarding Private Information and financial information and of the foreseeable consequences that would occur if Plaintiffs' and Class Members' PHI/PII and financial information was stolen, including the significant costs that would be placed on Plaintiffs and Class Members as a result of a breach of this magnitude. As detailed above, Defendant is a large, sophisticated organization with the resources to deploy robust cybersecurity protocols. It knew, or should have known, that the development and use of such protocols were necessary to fulfill its

[28] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson ed., 2012).
[29] *Id.* at 17.
[30] *Id.* at 28.
[31] *Id.*

statutory and common law duties to Plaintiffs and Class Members. Its failure to do so is, therefore, intentional, willful, reckless, and/or grossly negligent.

79. Defendant disregarded the rights of Plaintiffs and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that they did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiffs' and Class Members' Private Information and/or financial information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

PLAINTIFFS' EXPERIENCES

Plaintiff Nicole Toussaint

80. Plaintiff Nicole Toussaint is and at all times mentioned herein was an individual citizen residing in the State of Maine, in the city of Penobscot (Hancock County).

81. Plaintiff Toussaint is and was a former employee of Defendant at all times relevant to this Complaint.

82. Plaintiff Toussaint was employed at HBI as an Assistant Manager from the years 2012 through 2018.

83. Plaintiff Toussaint received a Notice of Data Breach Letter, related to HBI's Data Breach that is dated August 16, 2022. *See* attached as Exhibit A.

84. The Notice Letter that Plaintiff received states that her stolen information "may have included contact information; date of birth; financial account information; government issued identification numbers such as drivers' license numbers, passport information and social security numbers; and other information related to benefits and employment, including certain limited health information provided for employment-related purposes." *See* Ex. A. Her Notice Letter lacks specificity about the exact information breached.

85. Plaintiff Toussaint is especially alarmed by the amount of stolen or accessed PII listed on her letter, and even more by the fact that her Social Security number was identified as among the breached data on HBI's computer system.

86. Since the Data Breach, Plaintiff Toussaint monitors her financial accounts for as much as two hours per day. Having to spend this huge amount of time every week not only wastes her time as a result of HBI's negligence, but it also causes her great anxiety. She checks her credit reports periodically for any issues.

87. Plaintiff Toussaint also has to be vigilant about checking her emails for spam and other forms of identity theft. She now receives *many* spam emails and texts now and for the past months, and which she did not typically receive before. Specifically, she has been receiving about 3 or more strange spam emails weekly. These spam emails were not at all similar to ones she had received in the past. She thinks that they are related to HBI's Data Breach since she has only received this type of spam since about the time of the breach or after. The time she spends trying to block these unwanted communications is time that

she would rather use in other ways. She cannot figure out any other explanation than that it is related to HBI's Data Breach which included her Private Information.

88. Plaintiff Toussaint is aware that cybercriminals often sell Private Information, and that hers could be abused months or even years after this Data Breach. She is aware that she faces an imminent and substantial risk of identity theft as a result of HBI's Data Breach.

89. Had Plaintiff Toussaint been aware that HBI's computer systems were not secure, she would not have entrusted HBI with her personal data.

Plaintiff Veronica Roman

90. Plaintiff Veronica Roman is and at all times mentioned herein was an individual citizen residing in the State of California.

91. Plaintiff Roman is and was a former employee of Defendant at all times relevant to this Complaint.

92. Plaintiff Roman received a Notice of Data Breach Letter, related to HBI's Data Breach that is dated September 30, 2022. *See* attached as Exhibit B.

93. Like that of Plaintiff Toussaint, the Notice Letter that Plaintiff Roman received states that her stolen information "may have included contact information; date of birth; financial account information; government issued identification numbers such as drivers' license numbers, passport information and social security numbers; and other information related to benefits and employment, including certain limited health information provided for employment-related purposes." *See* Notice Letter, Ex. B. Her Notice Letter lacks specificity about the exact information breached.

94. Plaintiff Roman is especially alarmed by the amount of stolen or accessed PII listed on her letter, and even more by the fact that her Social Security number was identified as among the breached data on HBI's computer system.

95. Since the Data Breach, Plaintiff Roman monitors her financial accounts often–a task that is enormously wasteful and causes her great anxiety.

96. Plaintiff Roman also has to be vigilant about checking her emails for spam and other forms of identity theft. She now receives *many* spam communications and, for these past months, and which she did not typically receive before. The time she spends trying to block these unwanted communications is time that she would rather use in other ways.

97. Plaintiff Roman is aware that cybercriminals often sell Private Information, and that hers could be abused months or even years after this Data Breach. She is aware that she faces an imminent and substantial risk of identity theft as a result of HBI's Data Breach.

98. Had Plaintiff Roman been aware that HBI's computer systems were not secure, she would not have entrusted HBI with her personal data.

PLAINTIFFS' AND CLASS MEMBERS' INJURIES

99. To date, Defendant HBI has done absolutely nothing to compensate Plaintiffs and Class Members for the damages they sustained in the Data Breach.

100. Defendant HBI has merely offered identity monitoring services for a paltry 24 months through Experian IdentityWorks, an offer which expired just 3 months after offered, which is a tacit admission that its failure to protect their Private Information has

caused Plaintiffs and Class great injuries. *See* Exs. A, B. This two-year limitation –and its narrow enrollment window of about three months—is inadequate when victims are likely to face many years of identity theft.

101. HBI's offer fails to sufficiently compensate victims of the Data Breach, who commonly face multiple years of ongoing identity theft, and it entirely fails to provide any compensation for its unauthorized release and disclosure of Plaintiffs' and Class Members' Private Information, out of pocket costs, and the time they are required to spend attempting to mitigate their injuries.

102. Furthermore, Defendant HBI's credit monitoring offer and advice (see Exh. A) to Plaintiffs and Class Members squarely places the burden on Plaintiffs and Class Members, rather than on the Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach. Defendant merely sent instructions to Plaintiffs and Class Members about actions they can affirmatively take to protect themselves.

103. Plaintiffs and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

104. Plaintiffs' and Class Members' Private Information was compromised and exfiltrated by cyber-criminals as a direct and proximate result of the Data Breach.

105. Plaintiffs and Class Members were damaged in that their Private Information is now in the hands of cyber criminals, sold and potentially for sale for years into the future.

106. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at an actual, imminent, and substantial risk of harm from fraud and identity theft.

107. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach.

108. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

109. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members.

110. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

111. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

112. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

113. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of

out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

114. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

115. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

116. Defendant's delay in identifying and reporting the Data Breach caused additional harm. Early notification helps a victim of a Data Breach mitigate their injuries, and in the converse, delayed notification causes more harm and increases the risk of identity theft.

CLASS ACTION ALLEGATIONS

117. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated.

118. Plaintiffs propose the following Class definition(s), subject to amendment as appropriate:

> **National Class:**
> "All persons whose Private Information was compromised as a result of the May 2022 Data Breach and for which HBI provided notice since May 2022 (the "Class")."

California Subclass:
"All persons within the State of California whose Private Information was compromised as a result of the May 2022 Data Breach and for which HBI provided notice since May 2022 (the "Class")."

119. Excluded from the Class/Subclass are Defendant's officers and directors, and those of any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class/Subclass are members of the judiciary to whom this case is assigned, their families and members of their staff. Hereinafter the National Class and California Subclass are, collectively, referred to as the "Class" unless otherwise designated.

120. Plaintiffs hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

121. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. The exact number of Class Members is unknown to Plaintiffs at this time. HBI provided notice to state attorneys general that the Private Information of at least 75,106 individuals were accessed in the Data Breach.

122. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's conduct was per se negligent;

l. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

m. Whether Defendant was unjustly enriched;

n. Whether Defendant violated California privacy and business statutes;

o. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

p. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

123. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class member, was compromised in the Data Breach.

124. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

125. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

126. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution

of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

127. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

128. Finally, all Members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

First Count
Negligence
(On Behalf of Plaintiffs and All Class Members)

129. Plaintiffs re-alleges and incorporates the above allegations as if fully set forth herein.

130. Defendant HBI required Plaintiffs and Class Members to submit non-public personal information in order to obtain employment and employment benefits as well as other business services.

131. By collecting and storing this data in HBI's computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means

to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

132. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

133. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant HBI and its current and former employees and other individuals from whom it collected PII. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

134. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant was bound by industry standards to protect confidential Private Information.

135. Defendant breached its duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

f. Failing to timely and fully notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

136. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in businesses that employ many individuals.

137. It was therefore foreseeable that Defendant's failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

138. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

139. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members, upon information and belief, in an unsafe and unsecure manner.

140. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) to provide adequate, long-term credit monitoring to all Class Members.

Second Count
Negligence *Per Se*
(On Behalf of Plaintiffs and All Class Members)

141. Plaintiffs re-allege the above allegations as if fully set forth herein.

142. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

143. Defendant breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

144. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

145. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

146. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it failed to meet its duties, and that Defendant's breach would cause

Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

147. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

Third Count
Breach of Implied Contract
(On Behalf of Plaintiffs and All Class Members)

148. Plaintiffs re-allege the above allegations as if fully set forth herein.

149. When Plaintiffs and Class Members provided their Private Information to Defendant HBI in exchange for Defendant HBI's employment, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

150. Defendant HBI solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

151. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

152. Plaintiffs and Class Members provided their Private Information and their labor to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

153. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

154. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

155. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

156. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

157. As a direct and proximate result of Defendant's breach of the implied contracts, Class Members sustained damages as alleged herein, including the loss of the benefit of the bargain.

158. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

159. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

Fourth Count
Invasion of Privacy
(On Behalf of Plaintiffs and All Class Members)

160. Plaintiffs re-allege the above allegations as if fully set forth herein.

161. Plaintiffs and Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

162. Defendant's conduct as alleged above intruded upon Plaintiffs' and Class Members' seclusion under common law.

163. By intentionally failing to keep Plaintiffs' and Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiffs' and Class Members' privacy by:

a. Intentionally and substantially intruding into Plaintiffs' and Class Members' private affairs in a manner that identifies Plaintiffs and Class Members and that would be highly offensive and objectionable to an ordinary person; and

b. Intentionally publicizing private facts about Plaintiffs and Class Members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiffs and Class Members.

164. Defendant knew that an ordinary person in Plaintiffs' or Class Members' position would consider Defendant's intentional actions highly offensive and objectionable.

165. Defendant invaded Plaintiffs' and Class Members' right to privacy and intruded into Plaintiffs' and Class Members' private affairs by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

166. Defendant intentionally concealed from and delayed reporting to Plaintiffs and Class Members a security incident that misused and/or disclosed their Private Information without their informed, voluntary, affirmative, and clear consent.

167. The conduct described above was at or directed at Plaintiffs and the Class Members.

168. As a proximate result of such intentional misuse and disclosures, Plaintiffs' and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct amounted to a substantial and serious invasion of Plaintiffs' and Class Members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

169. In failing to protect Plaintiffs' and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiffs' and Class

Members' rights to have such information kept confidential and private. Plaintiffs, therefore, seek an award of damages on behalf of themselves and the Class.

Fifth Count
Unjust Enrichment
(On Behalf of Plaintiffs and All Class Members)

170. Plaintiffs re-allege the above allegations as if fully set forth herein. Plaintiffs bring this claim individually and on behalf of all Class Members. This count is plead in the alternative to the breach of contract count above.

171. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments for security of Private Information that was spent (or not spent) on behalf of Plaintiffs and the Class Members.

172. As such, a portion of the fruits of the labor of Plaintiffs and the Class Members is to be used to provide a reasonable level of data security, and the amount of money previously expended on computer and data security is known to Defendant, as is the amount that would have been required to maintain sufficient data security, had Defendant done so prior to this Data Breach.

173. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they provided labor and services to Defendant and/or its agents and in so doing were required to provide Defendant with their Private Information. In exchange, Plaintiffs and Class Members should have received from Defendant wages and benefits that were the subject of the transaction as well as a promise to protected their Private Information with adequate data security.

174. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from Class Members' labor and used the Private Information of Plaintiffs and Class Members for business purposes.

175. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

176. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

177. Defendant failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

178. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

179. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

180. Plaintiffs and Class Members have no adequate remedy at law.

181. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

182. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

183. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them.

Sixth Count
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiffs and All Class Members)

184. Plaintiffs re-allege the above allegations as if fully set forth herein. Plaintiffs bring this claim individually and on behalf of all Class Members.

185. Every contract has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

186. Plaintiffs and Class Members have complied with and performed all conditions of their contracts with Defendant.

187. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PHI/PII and financial information, failing to timely and accurately disclose the Data Breach to Plaintiffs and Class Members and continued acceptance of PHI/PII and financial information and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

188. Defendant acted in bad faith and/or with malicious motive in denying Plaintiffs and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

Seventh Count
Unfair Business Practices
(Cal. Bus. & Prof. Code §§ 17200, *et seq*.)
(On behalf of the California Subclass Only)

189. Plaintiff Roman re-alleges the above allegations as if fully set forth herein. Plaintiff Roman brings this claim individually and on behalf of all California Subclass Members.

190. Plaintiff Roman and California Subclass Members further bring this cause of action, seeking equitable and statutory relief to stop the misconduct of Defendant, as complained of herein.

191. Defendant has engaged in unfair competition within the meaning of Cal. Bus. & Prof. Code §§ 17200, *et seq.*, because Defendant's conduct is unlawful, unfair, and/or fraudulent, as herein alleged.

192. Plaintiff Roman, the California Subclass Members, and Defendant are each a "person" or "persons" within the meaning of § 17201 of the California Unfair Competition Law ("UCL").

193. The knowing conduct of Defendant, as alleged herein, constitutes an unlawful and/or fraudulent business practice, as set forth in Cal. Bus. & Prof. Code §§ 17200–17208. Specifically, Defendant conducted business activities while failing to comply with the legal mandates cited herein, including HIPAA. Such violations include, but are not necessarily limited to:

a. Failure to maintain adequate computer systems and data security practices to safeguard PHI/PII and financial information;

b. Failure to disclose that its computer systems and data security practices were inadequate to safeguard PHI/PII and financial information from theft;

c. Failure to timely and accurately disclose the Data Breach to Plaintiff Roman and California Subclass Members;

d. Continued acceptance of PHI/PII and financial information and storage of other personal information after Defendant knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach; and

e. Continued acceptance of PHI/PII and financial information and storage of other personal information after Defendant knew or should have known of the Data Breach and before they allegedly remediated the Data Breach.

194. Defendant knew, or should have known, that its computer systems and data security practices were inadequate to safeguard the PHI/PII and financial information of Plaintiff Roman and California Subclass Members, deter hackers, and detect a breach within a reasonable time and that the risk of a data breach was highly likely.

195. In engaging in these unlawful business practices, Defendant has enjoyed an advantage over its competition and a resultant disadvantage to the public and California Subclass Members.

196. Defendant's knowing failure to adopt policies in accordance with and/or adhere to these laws, all of which are binding upon and burdensome to Defendant's

competitors, engenders an unfair competitive advantage for Defendant, thereby constituting an unfair business practice, as set forth in Cal. Bus. & Prof. Code §§ 17200–17208.

197. Defendant has clearly established a policy of accepting a certain amount of collateral damage, as represented by the damages to Plaintiff Roman and California Subclass Members herein alleged, as incidental to its business operations, rather than accept the alternative costs of full compliance with fair, lawful, and honest business practices ordinarily borne by responsible competitors of Defendant and as set forth in legislation and the judicial record.

198. The UCL is, by its express terms, a cumulative remedy, such that remedies under its provisions can be awarded in addition to those provided under separate statutory schemes and/or common law remedies, such as those alleged in the other causes of action of this Complaint. *See* Cal. Bus. & Prof. Code § 17205.

199. Plaintiff Roman and California Subclass Members request that this Court enter such orders or judgments as may be necessary to enjoin Defendant from continuing its unfair, unlawful, and/or deceptive practices and to restore to Plaintiff Roman and California Subclass Members any money Defendant acquired by unfair competition, including restitution and/or equitable relief, including disgorgement of ill-gotten gains, refunds of moneys, interest, reasonable attorneys' fees, and the costs of prosecuting this class action, as well as any and all other relief that may be available at law or equity.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiffs and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and

j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: April 27, 2023

Respectfully submitted,

/s/ Gary E. Mason

Gary E. Mason*
Danielle Perry*
Lisa A. White*
MASON LLP
5335 Wisconsin Avenue NW, Suite 305
Washington, DC 20016
Tel: (202) 429-2290
gmason@masonllp.com
dperry@masonllp.com
lwhite@masonllp.com

Scott Edward Cole**
Cody A. Bolce**
COLE & VAN NOTE
555 12th Street, Suite 1725
Oakland, California 94607
Tel: (510) 891-9800
sec@colevannote.com
cab@colevannote.com

**by special appearance*
***special appearances to be filed*

Attorneys for Plaintiffs

Joel R. Rhine
Martin A. Ramey
RHINE LAW FIRM, P.C.
1612 Military Cutoff Road, Suite 300
Wilmington, NC 28403
Telephone: (910) 772-9960
Facsimile: (910) 772-9062
jrr@rhinelawfirm.com
mjr@rhinelawfirm.com

Rule 83.1(d) Counsel for Plaintiffs